IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/761,347	Confirmation No.: 3254
Applicant	:	Yoshihiro OBA	
Filed	:	January 22, 2004	
TC/A.U.	:	2141	
Examiner	:	Taylor, Nicholas	
Docket No.	:	3119-102	
Customer No.:		66458	

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

BRIEF ON APPEAL

Sir:

This is an appeal from the Examiner's final rejection of Claims 1-21 and 25-27 dated May 22, 2007. Claims 1-21 and 25-27 are currently pending in the application.

TABLE OF CONTENTS

REAL PARTY IN INTEREST:

The real parties in interest are: Toshiba America Research, Inc. and Telcordia Technologies, Inc.

RELATED APPEALS AND INTERFERENCES:

To the best of the undersigned's knowledge, there are no related appeals or interferences within the meaning of 37 C.F.R. §41.37(c)(1)(ii).

STATUS OF THE CLAIMS:

Claims 1-21 and 25-27 are pending in the current application. Claims 1-3, 5, 7-21, and 25-27 stand rejected, and Claims 4 and 6 stand as objected to as being allowable if placed in independent form.

A copy of these pending claims is found in the attached Claims Appendix.

STATUS OF THE AMENDMENTS:

No claims have been amended since the final office action of September 4, 2007.

SUMMARY OF THE CLAIMED SUBJECT MATTER:

Introduction:

For reference, some aspects of the present disclosure are described below. It is noted, however, that the following discussion does not limit the scope of the claims or otherwise limit the invention.

As noted in the disclosure, an IP-layer based model for network selection and multihoming is provided that enables a flexible and secure dynamic selection of one or more serving networks to use. The IP-layer based model according to one example consists of three phases. Network information is advertised to a

client node in a first phase, the client node is authenticated and authorized for use of an access router in the second phase, and a secure tunnel is established between the client node and the access router in the third phase.

Advertising network information is discussed with respect to the example on page 9 of the disclosure, where network layer protocols may be used to advertise serving network information to the client nodes on access network 101 (shown in, e.g., Fig. 1). When the routable networks are ISP or NAP networks, a provider identifier and provider name data pair may be advertised per each service provider. When the serving networks are VLANs, a VLAN identifier and a VLAN name may be advertised per VLAN. The identifier is a unique identifier that is used to identify the provider/VLAN and the name is a character string that represents the name of the provider/VLAN.

Thus, client nodes are able to selectively establish connectivity to one or more serving networks. In the example shown in Fig. 3 and discussed on page 17 of the disclosure, client node 10 is able to selective establish connectivity to one or more of the networks owned by ISP1, ISP2, ISP3 or NAP 301.

Summary:

With reference to independent claim 1, this claim recites a method of dynamically connecting a client node to a serving network, comprising the steps of: providing an access network to which a client node has a network connection; providing at least one access router having a network connection to said access network and having a network connection to at least one serving network; sending serving network provider advertising information to said client node;

receiving from said client node serving network provider information specifying a serving network to which said client node desires access; and establishing a communication tunnel between said client node and said access router through said access network, such that said client node is able to send and receive data packets to and from the serving network specified by said client node within said communication tunnel through said access network. In this

regard, reference is made to, e.g., the present specification at page 3, last paragraph to page 4, line 10, and pages 6-7, and FIGS. 1-2.

With reference to independent claim 25, this claim recites a method of connecting a client node to a serving network, comprising the steps of: providing an access router having a network connection to at least two serving networks; receiving from said client node serving network information specifying a serving network to which said client node desires to have access; establishing a communication tunnel between said client node and said access router through said access network, such that said client node is able to send and receive data packets to and from the serving network specified by said client node within said communication tunnel through said access network; and binding said communication tunnel to said specified serving network by using serving network information of said specified serving network as a security association identifier of said communication tunnel. In this regard, reference is made to, e.g., the present specification at page 4, last paragraph to page 5, line 3, and pages 6-7, and FIGS. 1-2.

With reference to claim 2, this claim further recites a method as set forth in claim 1, further comprising the step of authenticating said client node prior to establishing said communication tunnel. With reference to claim 3, this claim further recites a method as set forth in claim 1, further comprising the step of providing a second access router having a network connection to said access network and having network connections to at least two serving networks. With reference to claim 4, this claim further recites a method as set forth in claim 3, wherein when a serving network specified by said client node is associated with said second access router, said establishing step further comprises the step of binding said communication tunnel to said specified serving network associated with said second access router by using serving network information of said specified serving network as a security association identifier of said communication tunnel. With reference to claim 5, this claim further recites a

method as set forth in claim 1, wherein said access router has network connections to at least two serving networks, said method further comprising the step of establishing a second communication tunnel between said client node and said access router through said access network, such that said client node is able to selectively send and receive data packets to and from each of said two serving networks. With reference to claim 6, this claim further recites a method as set forth in claim 1, further comprising the step of providing a second access router having a network connection to said access network and a network connection to at least one serving network, said method further comprising the step of establishing a second communication tunnel between said client node and said second access router through said access network, such that said client node is able to selectively send and receive data packets to and from each of said serving networks associated with said access routers through said communication tunnels. With reference to claim 7, this claim further recites a method as set forth in claim 1, wherein said step of sending serving network provider advertising information comprises the step of using a PANA protocol. With reference to claim 8, this claim further recites a method as set forth in claim 1, wherein said step of sending serving network provider advertising information comprises the step of using a Router Discovery mechanism. With reference to claim 9, this claim further recites a method as set forth in claim 1, wherein said at least one serving network comprises an Internet Service Provider network. With reference to claim 10, this claim further recites a method as set forth in claim 1, wherein said at least one serving network comprises a Network Access Provider network. With reference to claim 11, this claim further recites a method as set forth in claim 1, wherein said at least one serving network comprises a VLAN network. With reference to claim 12, this claim further recites a method as set forth in claim 11, further comprising the step of providing a virtual access point in said VLAN serving network, through which a client node may connect directly to said VLAN serving network. With reference to claim 13, this claim

further recites a method as set forth in claim 1, wherein said access network comprises an IP access network. With reference to claim 14, this claim further recites a method as set forth in claim 1, wherein said access network comprises a VLAN access network. With reference to claim 15, this claim further recites, a method as set forth in claim 14, wherein said VLAN access network is partitioned into multiple VLAN access sub-networks. With reference to claim 16, this claim further recites a method as set forth in claim 14, further comprising the step of providing a virtual access point in said VLAN access network, through which a client node may connect to said VLAN access network. With reference to claim 17, this claim further recites a method as set forth in claim 1, wherein said client node connects to said access network via a remote network. With reference to claim 18, this claim further recites a method as set forth in claim 1, wherein the step of establishing said communication tunnel comprises the step of using an IPSec key management protocol. With reference to claim 19, this claim further recites a method as set forth in claim 1, wherein said client node is a mobile node, and said network connection of said client node to said access network is a wireless connection. With reference to claim 20, this claim further recites a method as set forth in claim 1, wherein said communication tunnel is a secure communication tunnel. With reference to claim 21, this claim further recites a method as set forth in claim 20, further comprising the step of establishing said secure communication tunnel using an IPSec key management protocol. With reference to claim 26, this claim further recites a method as set forth in claim 25, wherein said communication tunnel is a secure communication tunnel. With reference to claim 27, this claim further recites a method as set forth in claim 26, further comprising the step of establishing said secure communication tunnel using an IPSec key management protocol.

GROUND(S) OF REJECTION TO BE REVIEWED:

In the Office Action: 1) claims 1, 2, 5, 9, 10, 13, 17, 18, 20, 21, and 25-27 were rejected under 35 U.S.C. 102(e) over U.S. Patent Publication No. 2003/0145104 (Boden); 2) claim 3 was rejected under 35 U.S.C. 103(a) over Boden further in view of U.S. Patent Publication No. 2002/0196802 (Sakov); 3) claims 8, 11, 12, 14-16 and 19 were rejected under 35 U.S.C. 103(a) over Boden further in view of U.S. Patent Publication No. 2002/0069278 (Forslow); and 4) claim 7 was rejected under 35 U.S.C. 103(a) over Boden further in view of U.S. Patent Publication No. 2004/0019664 (Le). In addition, the finality of the final rejection is also under review.

ARGUMENTS:

Introductory Remarks:

On Page 3, Paragraph 3 (A) of the Office Action, the Examiner **incorrectly** asserts that "[a] tunnel is established between the client and access router such that the client is able to send data to and from the serving network specified within said communication tunnel (Boden, paragraphs 0073-0076; Figs. 5 and 12; see also use of AH, ESP, and other header information in paragraph 0062)." The Examiner's statement is **wrong**. In the Boden reference, a tunnel is a VPN connection between access routers (or Gateways in Boden), and **not** betweena client node and an access router. Accordingly, the VPN tunnelin Boden resides outside of any of the access networks whereas the tunnel in the present application resides within an access network.

The Prior Art Rejections are Improper

Claims 1, 2, 5, 9, 10, 13, 17, 18, 20, 21 and 25-27 stand rejected under 35 U.S.C. section 102(e) as being anticipated by Boden. This rejection is respectfully traversed.

As previously indicated, in the Office Action, the Examiner remarks that:

Boden teaches an incoming IPsec'd packet 100 containing network provider advertising information is received at the access router (Boden, paragraph 0062). The access router, in order to avoid a conflict due to overlapping remote address spaces, makes modifications to the incoming advertisement information so that conflicts do not occur on the destination network (see Boden paragraphs 0062-72 and the connection process detailed in Table 3 where gateway A modifies the advertisement information to be compatible with node A1's network). The access router then sends this information on to the client node. The client node responds if a connection is desired, and if so, a communication tunnel is established where the client node is able to send and receive data packets to the desired destination (Boden, see fig. 13 steps 188-194 where the advertising information in step 181 is forwarded to node A1 to establish the connection). Additionally, language limiting the prior art from making modifications to transferred network advertising information is not present in the rejected claims.

Claim 1:

Once again, it is most respectfully submitted that the rejection is improper with respect to claim 1 at least for the following reasons.

First, claim 1 recites, among other things, "establishing a communication tunnel between said client node and said access router through said access network, such that said client node is able to send and receive data packets to and from the serving network specified by said client node within said communication tunnel through said access network." However, as indicated above, on Page 3, Paragraph 3 (A) of the Office Action, the Examiner **incorrectly** asserts that "[a] tunnel is established between the client and access router such that the client is able to send data to and from the serving network specified within said communication tunnel (Boden, paragraphs 0073-0076; Figs. 5 and 12; see also use of AH, ESP, and other header information in paragraph 0062)." The Examiner's statement is **wrong**. In the Boden reference, a tunnel is a VPN connection between access routers (or Gateways in Boden), and **not** between a client node and an access router. Accordingly, the VPN tunnel in Boden resides outside of any of the access networks whereas the tunnel in the present

application resides within an access network.

Second, as also previously expressed, Boden fails to teach "sending serving network provider advertising information to said client node" as recited by claim 1. While the Examiner still has not named what portion of the packet 100 of Boden the Examiner considers to be network advertising information, in the above remarks, the Examiner indicates that the access router modifies the incoming advertisement information and sends the same on to the client node. Looking at the teachings of Boden, the modified portion of the packet 100 being sent to the node A1 corresponds to the *source IP address* (referred to in Boden as both "sip" and "src ip" – see paragraph 37, for example). However, as discussed in more detail below, the new source IP address (sip) sent to node A1 (what the Examiner identifies as the client node) is selected from a pool of administratively reserved IP addresses in gateway 52. Thus, the new source IP address provides no information regarding the serving network, let alone serving network provide advertising information.

Boden addresses the problem of remote networks having IP addresses which overlap with each other. Paragraph 0005 discusses an example where company A has a VPN gateway and wants to set up two VPN connections, one with a supplier and another with a west coast branch office, both having a system with an IP address of 1.2.3.4. Boden indicates two problems are caused by the overlapping addresses: **(1)** If two packets with IP address 1.2.3.4 from different 1.2.3.4 systems are both going to the same server in company A's network, how can the server tell them apart? **(2)** What does VPN gateway A do with a response packet with a destination IP address of 1.2.3.4 (in this example, should it go to the supplier's subnet or the branch office's subnet both with an IP address of 1.2.3.4)?

Boden addresses this problem by utilizing a VPN gateway with a network address translation (NAT) function. During *inbound* processing, the source IP address (sip) is translated using the VPN source-in NAT. For example, in Table 3,

step 188, "Gateway 52 changes the packet source IP 102 to lhs 114 100.123.254.5 and forwards it (packet 122) to node A1 47 (100.123.5.11)." Note that this lhs address is initially created within the bind table 58 by selecting an address from a pool of IP addresses (VPN NAT pool 60) which are administratively reserved within the A network (see paragraph 0049 and 0043).

In summary, during inbound processing, a source IP address (sip) is translated from the actual sip to a unique sip selected from an address pool. While this new unique sip may indeed be transmitted to node A1, it is not "serving network provider advertising information". *In fact, it provides no information whatsoever of the serving network provider, as it selected from a pool 60 (in VPN gateway 52) of administratively reserved IP addresses.* Having been selected from pool 60, this new source IP address (sip) could be associated with any external network, and there is no teaching that node A1 has any ability to assess anything about the serving network provider based on the new translated sip.

In addition, the remote networks may have overlapping addresses, as noted above. Therefore, if the original source IP address (sip) may be the same between several remote networks, it is unclear how even the unmodified original source IP address (sip) may be considered to qualify as "serving network provider advertising information".

Thus, because Boden fails to teach "sending serving network provider advertising information to said client node" as recited by claim 1, it is respectfully asserted for this reason the rejection is improper and should be withdrawn.

Third, as previously argued, claim 1 requires "establishing a communication tunnel between said client node and said access router through said access network". The rejection is improper as Boden fails to teach this recitation as well.

In the rejection, the Examine highlights network A (42) and node A1 in FIG. 4 as meeting the recitation of "providing an access network to which a client node

has a network connection. The Examiner highlights paragraph 0073-0076 and FIGS. 5 and 12 as teaching "establishing a communication tunnel between said client node and said access router through said access network." While FIG. 12 does illustrate a VPN tunnel 138, this tunnel is neither between "between said client node and said access router" (as identified by the Examiner, node A1 and VPN gateway A) nor "through said access network" (as identified by the Examiner, network A), and thus fails to meet the requirements of claim 1 for these additional reasons.

Examining Boden in more detail, "SA data 204 is used to process in 136 *outbound* packet 130 *into* VPN tunnel 138" (paragraph 0077 – emphasis added). This is confirmed by he labeling and arrows in FIG. 12. Thus, the tunnel referred to here is not from VPN gateway A through network A to node A1 (this is the *inbound* direction – see first line of paragraph 0062, e.g.), but from VPN gateway A to another external gateway (e.g., VPN gateway B or C in FIG. 4. See also paragraph 0004 of Boden, which clarifies that the tunnel connections (in Boden, a 'VPN connection') are from remote systems and gateways:

> Each gateway will support many independent VPN connections from many ***remote systems***, or ***remote gateways*** to smaller branch office networks, or suppliers (for example). The term 'VPN connection' is another term referring to what is generally called an 'IP Sec tunnel', ...
> (emphasis added).

The tunnel 138 of FIG. 12 thus appears to correspond in FIG. 5 to the line connection between VPN gateway A and VPN gateway B, or VPN gateway A and VPN gateway C.

In sum, the tunnel connections of Boden are not taught to be "between" node A1 and VPN gateway A nor "through" network A (42). Because, Boden also fails to teach "establishing a communication tunnel between said client node and said access route through said access network" as recited by claim 1, it is respectfully requested that the Examiner reconsider and withdraw this rejection.

Claims 2, 5, 13, 17, 18, 20 and 21:

Claims 2, 5, 13, 17, 18, 20 and 21 depend from claim 1 and are allowable at least for the reasons set forth above with respect to claim 1. In addition, these dependent claims also recite further combinations of features that are not taught or suggested by the cited references.

Claim 25:

First, claim 25 recites "receiving from said client node serving network information specifying a serving network to which said client node desires to have access." In the Amendment filed March 21, 2007, it was explained that paragraphs 62-72 of Boden relied upon by the Examiner to met this limitation, address actions of VPN gateway A 52 in connection with an *inbound* IPsec'd packet 100 – that is, from a source external to network A. There is no discussion in these paragraphs of "receiving from a client node" the recited serving network information as required by claim 25. Because Boden et al. fails to teach this limitation, it is respectfully requested that the Examiner reconsider and withdraws this rejection.

Second, claim 25 recites "establishing a communication tunnel between said client node and said access router through said access network." As noted above, the tunnel referred to in Boden is **not** between VPN gateway A and node A1, nor is it through network A. For these yet additional reasons, it is respectfully submitted that the rejection of claim 25 is improper.

Once again, it is respectfully submitted that the Examiner has not address this deficiency in the Office Action.

Claims 26 and 27:

Claims 26 and 27 depend from claim 25 and are allowable at least for the reasons set forth above with respect to claim 25. In addition, these dependent claims also recite further combinations of features that are not taught or suggested by the cited references.

Claims 3, 7, 8, 11, 12, 14-16 and 19:

In the Office Action, claim 3 was rejected under 35 U.S.C. 103(a) as being

unpatentable over Boden and Sakov (US PGPub 2002/0196802), claims 8, 11, 12, 14-16 and 19 were rejected under 35 U.S.C. 103(a) as being unpatentable over Boden and Forslow (US PGPub 2002/0069278), and claim 7 was rejected under 35 U.S.C. 103(a) as being unpatentable over Boden and Le (US PGPub 2004/0019664). These rejections are respectfully traversed.

Claims 3, 7, 8, 11, 12, 14-16, and 19 depend from claim 1. The Examiner alleges the teachings of Sakov, Forslow and Le teach limitations of the dependent claims which are missing from Boden, and asserts these limitations would have been obvious to use with the system of Boden et al. However, these secondary references fail to correct the deficiencies of Boden et al. noted above with respect to claim 1. Thus, the applicants respectfully request the Examiner to reconsider and withdraw these rejections.

It is again most respectfully submitted that the Examiner's characterization of certain elements of Boden without argument. However, any lack of argument should not be used to infer agreement.

Finality of Office Action:

Once again, the undersigned respectfully submits that the Examiner has improperly made issued a Final Office Action. In the event that the Examiner maintains the rejection, it is respectfully requested that such be issued in a new non-final Office Action. MPEP section 706.07(a) states:

> Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims nor based on information submitted in an information disclosure statement.

In the final Office Action, the Examiner has introduced a new ground of rejection, rejecting the claims under 35 U.S.C. section 102(e). This is the first time this rejection has been made. The Examiner asserts that the finality is still proper since the previous rejection was a result of a typographical error. Whether this is relevant or not, that the rejection of the previous office action was a result of a

typographical error was **not** have been apparent to the Applicant, especially in view of the consistent reference to 35 U.S.C. section 102(b) throughout the rejection. For example, paragraph 7 sets forth the entire text of 35 U.S.C. section 102(b) and paragraph 8 consistently sets forth the rejection under 35 U.S.C. section 102(b). In any event, the rejection in the last Office Action of May 22, 2007 is under 35 U.S.C. section 102(e). As this ground of rejection had not been made until the final Office Action, it is a new ground of rejection. Therefore, since the Examiner has introduced "a new ground of rejection that is neither necessitated by applicant's amendment of the claims nor based on information submitted in an information disclosure statement" it is respectfully asserted that the finality is improper and requested the Examiner reconsider and withdraw the finality of the Office Action.

Conclusion

Applicant respectfully submits that the present application is in condition for allowance, which action is courteously requested. Please charge any shortage in fees that may be due in connection with the filing of this paper, including Extension of Time fees, to Deposit Account 50-4080.

Respectfully submitted,

/Stephen B. Parker, Reg. No. 36,631/

Stephen B. Parker
Registration No. 36,631
WATCHSTONE P&D, pllc
1250 Connecticut Ave., N.W.
Suite 700
Washington, DC 20036-2657
(202) 419-1518
(202) 318-4261

Dated: February 25, 2008

CLAIMS APPENDIX

1. A method of dynamically connecting a client node to a serving network, comprising the steps of:

providing an access network to which a client node has a network connection;

providing at least one access router having a network connection to said access network and having a network connection to at least one serving network;

sending serving network provider advertising information to said client node;

receiving from said client node serving network provider information specifying a serving network to which said client node desires access; and

establishing a communication tunnel between said client node and said access router through said access network, such that said client node is able to send and receive data packets to and from the serving network specified by said client node within said communication tunnel through said access network.

2. A method as set forth in claim 1, further comprising the step of authenticating said client node prior to establishing said communication tunnel.

3. A method as set forth in claim 1, further comprising the step of providing a second access router having a network connection to said access network and having network connections to at least two serving networks.

4. A method as set forth in claim 3, wherein when a serving network specified by said client node is associated with said second access router, said establishing step further comprises the step of binding said communication tunnel to said specified serving network associated with said second access

router by using serving network information of said specified serving network as a security association identifier of said communication tunnel.

5. A method as set forth in claim 1, wherein said access router has network connections to at least two serving networks, said method further comprising the step of establishing a second communication tunnel between said client node and said access router through said access network, such that said client node is able to selectively send and receive data packets to and from each of said two serving networks.

6. A method as set forth in claim 1, further comprising the step of providing a second access router having a network connection to said access network and a network connection to at least one serving network, said method further comprising the step of establishing a second communication tunnel between said client node and said second access router through said access network, such that said client node is able to selectively send and receive data packets to and from each of said serving networks associated with said access routers through said communication tunnels.

7. A method as set forth in claim 1, wherein said step of sending serving network provider advertising information comprises the step of using a PANA protocol.

8. A method as set forth in claim 1, wherein said step of sending serving network provider advertising information comprises the step of using a Router Discovery mechanism.

9. A method as set forth in claim 1, wherein said at least one serving network comprises an Internet Service Provider network.

10. A method as set forth in claim 1, wherein said at least one serving network comprises a Network Access Provider network.

11. A method as set forth in claim 1, wherein said at least one serving network comprises a VLAN network.

12. A method as set forth in claim 11, further comprising the step of providing a virtual access point in said VLAN serving network, through which a client node may connect directly to said VLAN serving network.

13. A method as set forth in claim 1, wherein said access network comprises an IP access network.

14. A method as set forth in claim 1, wherein said access network comprises a VLAN access network.

15. A method as set forth in claim 14, wherein said VLAN access network is partitioned into multiple VLAN access sub-networks.

16. A method as set forth in claim 14, further comprising the step of providing a virtual access point in said VLAN access network, through which a client node may connect to said VLAN access network.

17. A method as set forth in claim 1, wherein said client node connects to said access network via a remote network.

18. A method as set forth in claim 1, wherein the step of establishing said communication tunnel comprises the step of using an IPSec key management protocol.

19. A method as set forth in claim 1, wherein said client node is a mobile node, and said network connection of said client node to said access network is a wireless connection.

20. A method as set forth in claim 1, wherein said communication tunnel is a secure communication tunnel.

21. A method as set forth in claim 20, further comprising the step of establishing said secure communication tunnel using an IPSec key management protocol.

25. A method of connecting a client node to a serving network, comprising the steps of:

providing an access router having a network connection to at least two serving networks;

receiving from said client node serving network information specifying a serving network to which said client node desires to have access;

establishing a communication tunnel between said client node and said access router through said access network, such that said client node is able to send and receive data packets to and from the serving network specified by said client node within said communication tunnel through said access network; and

binding said communication tunnel to said specified serving network by using serving network information of said specified serving network as a security association identifier of said communication tunnel.

26. A method as set forth in claim 25, wherein said communication tunnel is a secure communication tunnel.

27. A method as set forth in claim 26, further comprising the step of establishing said secure communication tunnel using an IPSec key management protocol.

RELATED PROCEEDINGS APPENDIX

There are no other related proceedings.